CLAIMS

1. An electronic document for reproduction of a corresponding printed document capable of having the legitimacy of said electronic document protected, said printed document being a printed version of said electronic document, said electronic document including:

content of an original document in electronic form;

a content digest for said content said original document in electronic form;

an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

an optically sensitive or sensible component added to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

2. The electronic document according to claim 1, further including a watermark in said e-seal for embedding said content digest in said visible seal.

3. The electronic document according to claim 2, wherein said content digest is encrypted prior to watermarking said visible seal.

4. The electronic document according to claim 3, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both.

5. The electronic document according to claim 1, wherein said content digest is a condensed representation of said original document generated by a step selected from the group consisting of:

hashing said content using a secure hashing process;

selecting key items of said content; and

extracting features of said content.

6. The electronic document according to claim 1, wherein said content digest is a condensed representation of said original document generated by block-wise digest derivation applied to said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

7. The electronic document according to claim 1, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

8. The electronic document according to claim 1, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

9. The electronic document according to claim 1, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

10. The electronic document according to claim 1, further including a second e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

11. The electronic document according to claim 1, further including an imperceptible watermark embedded in said e-seal for protecting ownership of the authority of said e-seal.

12. A printed document reproduced from an electronic document capable of having the legitimacy of said printed document protected, said printed document being a printed version of said electronic document, said printed document including:

rendered content of an original document;

an electronic seal or e-seal for authenticating said original document rendered in said printed document, said e-seal including a visible seal of an authority and a content digest for said content of said original document embedded in said visible seal;

an optically sensitive or sensible component rendered in said authenticated document using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

13. The printed document according to claim 12, further including a watermark in said rendered e-seal for embedding said content digest in said visible seal.

14. The printed document according to claim 13, wherein said content digest is encrypted prior to watermarking said visible seal.

15. The printed document according to claim 14, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both.

16. The printed document according to claim 12, wherein said content digest is a condensed representation of said original document generated by a step selected from the group consisting of:

hashing said content using a secure hashing process;

selecting key items of said content; and

extracting features of said content.

17. The printed document according to claim 12, wherein said content digest is a condensed representation of said original document generated by block-wise digest derivation applied to said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

18. The printed document according to claim 12, wherein said rendered visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

19. The printed document according to claim 12, wherein said optically sensitive or sensible component includes a serial number for said printed document.

20. The printed document according to claim 12, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

21. The printed document according to claim 12, further including a second rendered e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

22. The printed document according to claim 12, further including an imperceptible watermark embedded in said e-seal for protecting ownership of the authority of said e-seal.

23. A method of protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said method including the steps of:

generating a content digest for an original document in electronic form;

authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

24. The method according to claim 23, wherein said authenticating step includes the step of watermarking said visible seal with said content digest to embed said content digest in said visible seal.

25. The method according to claim 24, wherein said authenticating step includes the step of encrypting said content digest prior to watermarking said visible seal.

26. The method according to claim 25, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both..

27. The method according to claim 23, wherein said content digest is a condensed representation of said original document generated by a step selected from the group consisting of:

hashing said content using a secure hashing process;

selecting key items of said content; and

extracting features of said content.

28. The method according to claim 23, wherein said content digest is a condensed representation of said original document generated by block-wise digest derivation applied to said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

29. The method according to claim 23, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

30. The method according to claim 23, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

31. The method according to claim 23, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

32. The method according to claim 23, further including a second e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

33. The method according to claim 23, further including the step of embedding an imperceptible watermark in said e-seal for protecting ownership of the authority of said e-seal.

34. An apparatus for protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said apparatus including:

means for generating a content digest for an original document in electronic form;

means for authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

means for adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

35. The apparatus according to claim 34, wherein said authenticating means includes means for watermarking said visible seal with said content digest to embed said content digest in said visible seal.

36. The apparatus according to claim 35, wherein said authenticating means includes means for encrypting said content digest prior to watermarking said visible seal.

37. The apparatus according to claim 36, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both.

38. The apparatus according to claim 34, wherein said content digest is a condensed representation of said original document generated by means selected from the group consisting of:

means for hashing said content using a secure hashing process;

means for selecting key items of said content; and

means for extracting features of said content.

39. The apparatus according to claim 34, wherein said content digest is a condensed representation of said original document generated by means for block-wise digest derivation of said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

40. The apparatus according to claim 34, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

41. The apparatus according to claim 34, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

42. The apparatus according to claim 34, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

43. The apparatus according to claim 34, further including a second e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

44. The apparatus according to claim 34, further including means for embedding an imperceptible watermark in said e-seal for protecting ownership of the authority of said e-seal.

45. A computer program product having a computer usable medium having a computer readable program code means embodied therein for protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said computer program product including:

computer readable program code means for generating a content digest for an original document in electronic form;

computer readable program code means for authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

computer readable program code means for adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

46. The computer program product according to claim 45, wherein said computer readable program code means for authenticating includes computer readable program code means for watermarking said visible seal with said content digest to embed said content digest in said visible seal.

47. The computer program product according to claim 46, wherein said computer readable program code means for authenticating includes computer readable program code means for encrypting said content digest prior to watermarking said visible seal.

48. The computer program product according to claim 47, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both..

49. The computer program product according to claim 45, wherein said content digest is a condensed representation of said original document generated by computer readable program code means selected from the group consisting of:

computer readable program code means for hashing said content using a secure hashing process;

computer readable program code means for selecting key items of said content; and

computer readable program code means for extracting features of said content.

50. The computer program product according to claim 45, wherein said content digest is a condensed representation of said original document generated by computer readable program code means for block-wise digest derivation of said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

51. The computer program product according to claim 45, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

52. The computer program product according to claim 45, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

53. The computer program product according to claim 45, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

54. The computer program product according to claim 45, further including a second e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

55. The computer program product according to claim 45, further including computer readable program code means for embedding an imperceptible watermark in said e-seal for protecting ownership of the authority of said e-seal.

56. A system utilising a network for protecting the legitimacy of an electronic document and a corresponding printed document, said printed document being a printed version of said electronic document, said system including:

means for generating a content digest for an original document in electronic form;

means for authenticating said original document in electronic form using an electronic seal or e-seal, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

means for adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document.

57. The system according to claim 56, wherein said authenticating means includes means for watermarking said visible seal with said content digest to embed said content digest in said visible seal.

58. The system according to claim 57, wherein said authenticating means includes means for encrypting said content digest prior to watermarking said visible seal.

59. The system according to claim 58, wherein at least one of an embedding address, shape, and boundary of said watermark is a key for encrypting said content digest, watermarking said e-seal, or both.

60. The system according to claim 56, wherein said content digest is a condensed representation of said original document generated by means selected from the group consisting of:

means for hashing said content using a secure hashing process;
means for selecting key items of said content; and
means for extracting features of said content.

61. The system according to claim 56, wherein said content digest is a condensed representation of said original document generated by means for block-wise digest derivation of said content, each block having a predetermined size and shape, said content digest including an array of labels with each label being dependent upon a classification of a corresponding block of said content.

62. The system according to claim 56, wherein said visible seal includes at least one of a document header, a logo or artwork, a graphical symbol, and a signature.

63. The system according to claim 56, wherein said optically sensitive or sensible component includes a serial number for said electronic document.

64. The system according to claim 56, wherein said electronic document includes:

at least one of two or more pages and multimedia information in said content; and

one or more landmarks for locating at least one of said content, said e-seal, and other document components.

65. The system according to claim 56, further including a second e-seal having:

content for said second e-seal including said content of said original document and said (first) e-seal; and

a visible seal of an authority and a content digest dependent upon said content of said second e-seal embedded in said visible seal.

66. The system according to claim 56, further including a trusted printing or reproduction device for printing said authenticated document containing said optical sensitive or sensible component.

67. The system according to claim 66, wherein said trusted printing or reproduction device is accessible via said network and is remotely located from one or more of the other components of said system.

68. The system according to claim 56, further including means for embedding an imperceptible watermark in said e-seal for protecting ownership of the authority of said e-seal.

69. A system for protecting the legitimacy of an electronic document and a corresponding printed document, said system including:

means for generating an authenticated electronic document, said authenticated electronic document including content of an original document in electronic form, an electronic seal or e-seal for authenticating said original document in electronic form,

said e-seal including a visible seal of an authority and a content digest embedded in said e-seal;

means for generating an optically sensitive or sensible component added to said authenticated electronic document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

means for verifying the legitimacy of said authenticated electronic document;

means for printing said authenticated electronic document and said optically sensitive component using said trusted printing process dependent upon said verifying means to provide an authenticated printed document.

70. The system according to claim 69, wherein said legitimacy verifying means includes means for verifying a watermarked digest of content against a corresponding one of one or more e-seals included in said authenticated electronic document.

71. The system according to claim 70, wherein said legitimacy verifying means further includes means for locating and verifying one or more e-seals in said authenticated electronic document.

72. The system according to claim 70, wherein said legitimacy verifying means further includes means for verifying the validity of each of one or more e-seals included in said authenticated electronic document.

73. The system according to claim 69, further including:

means for verifying the legitimacy protection of said authenticated printed document based on said electronic document.

74. The system according to claim 73, wherein said means for verifying the legitimacy protection said authenticated printed document further including:

means for visually inspecting said visual seal of each of said one or more e-seals;

means for verifying said optically sensitive component of said authenticated printed document;

means for scanning said authenticated printed document and extracting a watermark from each of said one or more e-seals; and

means for extracting a content digest from each of said watermarks and verifying said extracted content digest.

75. A method for protecting the legitimacy of an electronic document and a corresponding printed document, said method including the steps of:

generating an authenticated electronic document, said authenticated electronic document including content of an original document in electronic form, an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and a content digest embedded in said e-seal;

generating an optically sensitive or sensible component added to said authenticated electronic document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

verifying the legitimacy of said authenticated electronic document;

printing said authenticated electronic document and said optically sensitive component using said trusted printing process dependent upon said verifying step to provide an authenticated printed document.

76. The method according to claim 75, wherein said legitimacy verifying step includes the step of verifying a watermarked digest of content against a corresponding one of one or more e-seals included in said authenticated electronic document.

77. The method according to claim 76, wherein said legitimacy verifying step further includes the steps of locating and verifying one or more e-seals in said authenticated electronic document.

78. The method according to claim 76, wherein said legitimacy verifying step further includes the step of verifying the validity of each of one or more e-seals included in said authenticated electronic document.

79. The method according to claim 75, further including a step of verifying the legitimacy protection of said authenticated printed document based on said electronic document.

80. The method according to claim 79, wherein said step for verifying the legitimacy protection said authenticated printed document further includes the steps of:

visually inspecting said visual seal of each of said one or more e-seals;

verifying said optically sensitive component of said authenticated printed document;

scanning said authenticated printed document and extracting a watermark from each of said one or more e-seals; and

extracting a content digest from each of said watermarks and verifying said extracted content digest.

81. A computer program product having a computer usable medium having a computer readable program code means embodied therein for protecting the legitimacy of an electronic document and a corresponding printed document, said computer program product including:

computer readable program code means for generating an authenticated electronic document, said authenticated electronic document including content of an original document in electronic form, an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and a content digest embedded in said e-seal;

computer readable program code means for generating an optically sensitive or sensible component added to said authenticated electronic document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

computer readable program code means for verifying the legitimacy of said authenticated electronic document;

computer readable program code means for printing said authenticated electronic document and said optically sensitive component using said trusted printing process dependent upon said computer readable program code means means for verifying to provide an authenticated printed document.

82. The computer program product according to claim 81, wherein said computer readable program code means for verifying legitimacy includes computer readable program code means for verifying a watermarked digest of content against a corresponding one of one or more e-seals included in said authenticated electronic document.

83. The computer program product according to claim 82, wherein said computer readable program code means for legitimacy verifying further includes computer readable program code means for locating and verifying one or more e-seals in said authenticated electronic document.

84. The computer program product according to claim 82, wherein said computer readable program code means for legitimacy verifying further includes computer readable program code means for verifying the validity of each of one or more e-seals included in said authenticated electronic document.

85. The computer program product according to claim 81, further including:

computer readable program code means for verifying the legitimacy protection of said authenticated printed document based on said electronic document.

86. The computer program product according to claim 85, wherein said computer readable program code means for verifying the legitimacy protection said authenticated printed document further including:

computer readable program code means for visually inspecting said visual seal of each of said one or more e-seals;

computer readable program code means for verifying said optically sensitive component of said authenticated printed document;

computer readable program code means for scanning said authenticated printed document and extracting a watermark from each of said one or more e-seals; and

computer readable program code means for extracting a content digest from each of said watermarks and verifying said extracted content digest.

87. A method of trusted document delivery via a network, said method including the steps of:

establishing a secure communication link between parties at one or more locations;

verifying the identity of each party;

providing means for a party to sign an original document;

protecting the legitimacy of a signed document in electronic form, said protected signed document including content of an original document in electronic form, a content digest for said content of said original document in electronic form, and an electronic seal or e-seal for authenticating said original document in electronic form, said e-seal including a visible seal of an authority and said content digest embedded in said visible seal;

sending a protected, signed electronic document from a sending party at a first location to a receiving party at a second remote location of said network;

notifying said receiving party of said sent protected electronic document;

receiving said sent protected electronic document at said second remote location of said network; and

sending a receipt of said sent protected electronic document to said sending party at said first location.

88. The method according to claim 87, further including the steps of:

verifiying the legitimacy of said sent protected electronic document at said second remote location of said network to ensure the legitimacy of a document to be printed;

adding an optically sensitive or sensible component to said authenticated document for printing using a trusted printing process, said optically sensitive or sensible component containing information for indicating copying or modification of said printed document in a copy or modified version of said printed document;

printing a copy of said protected electronic document using a trusted printing process.

89. The method according to claim 87, further being a certification / notarization method including the steps of:

establishing a secure network with an issuer, an owner and the recipient of the document;

obtaining an electronic document for an owner and assigning a trust statement to the document;

delivering a trusted copy of the document to the recipient.

90. The method according to claim 89, further including the step of providing an electronic safe deposit box for storage of electronic certificates.

91. The method according to claim 87, further being an electronic check transacting method including the steps of:

establishing a secure network link from a service center to a payee, a payer, and one or more respective banks;

signing an electronic check and sending said check to the payee, said check being said signed electronic document;

claiming said check for the payee;

clearing the transaction; and

refusing the payment if the check is not legitimate.

92. The method according to claim 87, being a method for signing of documents with multiple signing parties including the step of:

establishing a secure network link between a service center and signers;

freezing an agreed version of said electronic document; and

signing said electronic document in either a serial or parallel manner.

93. The method according to claim 87, further including the step of converting said original document in printed form to said original document electronic form using a scanning process.

94. The method according to claim 87, further including the step of verifying the legitimacy of said sent protected electronic at a location of said network.

95. The method according to claim 87, further including the step of providing means for a party to sign said original document.